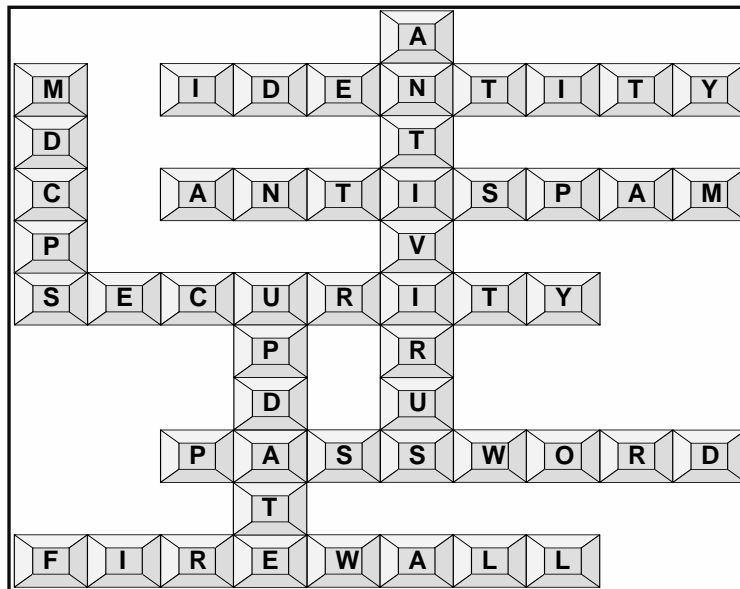


Internal Audit Report

Miami-Dade County Public Schools Office of Management and Compliance Audits



NETWORK AND INFORMATION SECURITY INFORMATION TECHNOLOGY SERVICES INFRASTRUCTURE AND SYSTEMS SUPPORT AREA I – SELECTED SCHOOL SITES



Some trends in data and network security matters noted suggest the need for consistency in applying leading practices and monitoring compliance with the M-DCPS Network Security Standards.

May 2011

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA

Ms. Perla Tabares Hantman, Chair
Dr. Lawrence S. Feldman, Vice Chair
Dr. Dorothy Bendross-Mindingall
Mr. Carlos L. Curbelo
Mr. Renier Diaz de la Portilla
Dr. Wilbert "Tee" Holloway
Dr. Martin Karp
Dr. Marta Pérez
Ms. Raquel A. Regalado

Mr. Alberto M. Carvalho
Superintendent of Schools

Mr. Jose F. Montes de Oca, CPA
Chief Auditor
Office of Management and Compliance Audits

Contributors to This Report:

Audit Performed by:
Mr. Luis Baluja
Ms. Dina Pearlman, CISA, CIA

Audit Reviewed by:
Mr. Trevor L. Williams, CPA

Supervised by:
Mr. Trevor L. Williams, CPA





Miami-Dade County Public Schools

giving our students the world

Superintendent of Schools

Alberto M. Carvalho

Chief Auditor

Jose F. Montes de Oca, CPA

Miami-Dade County School Board

Perla Tabares Hantman, Chair

Dr. Lawrence S. Feldman, Vice Chair

Dr. Dorothy Bendross-Mindingall

Carlos L. Curbelo

Renier Diaz de la Portilla

Dr. Wilbert "Tee" Holloway

Dr. Martin Karp

Dr. Marta Pérez

Raquel A. Regalado

May 11, 2011

Members of the School Board of Miami-Dade County, Florida

Members of the School Board Audit Committee

Mr. Alberto M. Carvalho, Superintendent of Schools

Ladies and Gentlemen:

In accordance with the approved Audit Plan for the 2010-11 Fiscal Year, we have completed an Information Technology audit at various schools aligned within Information Technology Services (ITS) Infrastructure and Systems Support (ISS) Area I to assess network security and to evaluate the mechanisms in place at those schools to protect critical systems and data.

This report includes 20 of the 60 schools that are under the auspices of ITS ISS Area I. An assessment of the remaining 40 schools within ITS ISS Area I will be reported at a future date. This is the second in a series of reports of this nature to be completed at Miami-Dade County Public Schools (M-DCPS).

Our audit concludes that while general measures for compliance with some standards of the M-DCPS Network Security Standards (NSS) are in place at the schools reported on in this support area, there is a need for greater compliance with these standards and other best practices. Admittedly, 100% compliance is difficult to achieve and is not expected. Further, the NSS provides the first line of defense and is augmented by other layers of protection. Our audit found that certain trends identified during the course of this audit disclosed areas that can greatly benefit from fuller compliance with the NSS and additional standardization across the M-DCPS network, as well as increased oversight of school-based technology support staff.

Our findings and recommendations were discussed with management whose responses, along with explanations, are included herein. We would like to acknowledge the administration's positive, prompt and efficient response to our recommendations. We would also like to thank management for the cooperation and courtesies extended to our staff during the audit.

Sincerely,

Jose F. Montes de Oca, CPA, Chief Auditor
Office of Management and Compliance Audits

Office of Management and Compliance Audits

School Board Administration Building • 1450 N.E. 2nd Ave. • Suite 415 • Miami, FL 33132

305-995-1436 • 305-995-1331 (FAX) • <http://mca.dadeschools.net>

TABLE OF CONTENTS

	Page Number
EXECUTIVE SUMMARY	1
INTERNAL CONTROLS	3
BACKGROUND	4
ORGANIZATIONAL CHART	6
OBJECTIVES, SCOPE AND METHODOLOGY	7
FINDINGS AND RECOMMENDATIONS	
1. Reconcile School Site Active Directory Computer Accounts.....	9
2. Antivirus Software Needs to Be Installed on All Computers.....	11
3. Computers Need To Be Password-Protected After User Login	13
4. Non-Standard Local Administrator Accounts Are Found Throughout Some Schools' Networks.....	15
5. Some Computers Are Named in a Manner That Increases Vulnerability	18
6. Servers Need To Be Routinely Backed Up	19
7. Perform Reviews For the Presence of Unauthorized Wireless Access Points and Document the Results	21
MANAGEMENT'S RESPONSE	23

EXECUTIVE SUMMARY

The Miami-Dade County Public Schools (M-DCPS) system comprises over 350 schools, which principal business is to educate students in a safe environment. In carrying out this mission, each school executes and manages various business processes, transactions and data across the District's network infrastructure. Both the large number of school sites and their sprawling placement throughout the county make keeping network resources available at all times a significant undertaking for the District's IT department.

Our audit objectives focused on assessing each school's compliance with the District's policies as described in the M-DCPS Network Security Standards (NSS) document, which is the first line of defense against security threats, and with industry best practices. This is the second in a series of reports of this nature to be completed at M-DCPS.

The increase in the potential risk of exposure and the vulnerability of data in today's environment make it incumbent upon the District to be proactive in protecting its student, business and employee data and the systems supporting these processes. The findings and corresponding recommendations presented in this report are intended to assist the District in protecting these resources.

OVERVIEW OF FINDINGS

- **Administrator's awareness of the M-DCPS NSS and the need to migrate all computers to the DADESCHOOLS domain and to ensure that critical software updates are installed on these machines are evident. However, all computers did not have the required anti-virus software installed.**
- **School site Active Directory computer accounts should be reconciled to BixFix. Thirteen of the 20 locations reviewed (or 65%) have not reconciled AD.**
- **Computers should be password-protected after user login. Not all non-student computers were password-protected.**
- **While computers generally contained the required minimum accounts, various non-standard Local Administrator accounts are found throughout 10 of the 20 (or 50%) school networks tested.**
- **Computer names were found to begin with the four-digit location number as required, but some computers tested at five schools were named in a manner that increases vulnerability to attacks.**
- **Although some documentation that is typical for a disaster recovery plan was maintained, routine backups of servers was not being done at four of the 20 (or 20%) schools tested.**
- **Review for the presence of unauthorized wireless access points needs to be consistently performed and documented.**

Our findings indicate that adequate management of network resources is generally taking place. However, certain trends identified during the course of this audit disclosed areas that can greatly benefit from fuller compliance with the NSS and additional standardization across the M-DCPS network, as well as increased oversight of school-based technology support staff. Admittedly, 100% compliance is difficult to achieve and is therefore, not expected. There were other less critical matters discussed with management that are not reported herein.

Based on our observations, we have made eight (8) recommendations. Our detailed findings begin on page 9. We would like to thank the administration for their cooperation and courtesies extended to our staff during the audits.

INTERNAL CONTROLS

The charts below summarize our overall assessment of network, data and systems security found at the 20 schools reported on herein that are under the auspices of ISS Support Area I. An assessment of the remaining 40 schools within ISS Support Area I will be reported at a future date.

INTERNAL CONTROLS RATING			
CRITERIA	SATISFACTORY	NEEDS IMPROVEMENT	INADEQUATE
Process Controls	X		
Policy & Procedures Compliance		X	
Effect	X		
Information Risk		X	
External Risk		X	

INTERNAL CONTROLS LEGEND			
CRITERIA	SATISFACTORY	NEEDS IMPROVEMENT	INADEQUATE
Process Controls	Effective	Opportunities exist to improve effectiveness.	Do not exist or are not reliable.
Policy & Procedures Compliance	In compliance	Non-Compliance Issues exist.	Non - compliance issues are pervasive, significant, or have severe consequences.
Effect	Not likely to impact operations or program outcomes.	Impact on outcomes contained.	Negative impact on outcomes.
Information Risk	Information systems are reliable.	Data systems are mostly accurate but can be improved.	Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions.
External Risk	None or low.	Potential for damage.	Severe risk of damage.

BACKGROUND

M-DCPS currently utilizes approximately 125,000 computers at over 400 different physical locations across an enterprise-level network. This large network connects students, teachers, administrators and parents with a vast amount of information and educational tools. For instance, student's grades and attendance are reported via an electronic grade book system. Business transactions such as procurement of goods and services and employee payroll are also processed on the District's network. Webinars, which allow Principals to attend important district meetings without having to leave the school campus, where they are most needed, are accessed through the network. Parents and students can review student's progress using the District's portals. These and many other extremely critical district functions rely on the availability of a robust network with properly managed resources and equipment.

Technical Support Technicians (TST's) are the primary source of technical support at each school site. On June 17, 2009, the School Board of Miami-Dade County approved board agenda item D-26, which realigned the reporting structure for TST's (then known as School-Based Technicians) from the school-site administrator (i.e., Principal) to a more centralized model under ITS. Under this model, technicians typically are assigned to one or more schools and also provide assistance to other nearby schools, as needed. Infrastructure and Systems Support (ISS) is a subdivision of ITS and is responsible for managing TST's and providing all school site IT support. ISS has created six support areas, each maintained by a technical team that serves about 55-60 schools. ISS Support Area I (60 schools) is staffed as follows:

<i>ISS Support Area I</i> (March 2011)	
Title	Quantity
Technical Support Technician (TST): <ul style="list-style-type: none">• Microsystems Technician (MST)• Computer Specialist (CS)• Computer Technician (CT)	41
Network Data Communication Specialist (NDCS)	3
Network Analyst (NA , Administrator)	1
Project Manager (PM , Administrator)	1
TOTAL	46

Technical Support Technicians typically provide routine technology support at schools, including help desk-related services, computer and equipment repair, and the managing of network resources such as printers, servers, software and data storage. Other issues, such as infrastructure equipment problems that cannot be handled by the on-site technician are escalated to NDCS staff. TSTs and NDCS report to a Project Manager through a Network Analyst.

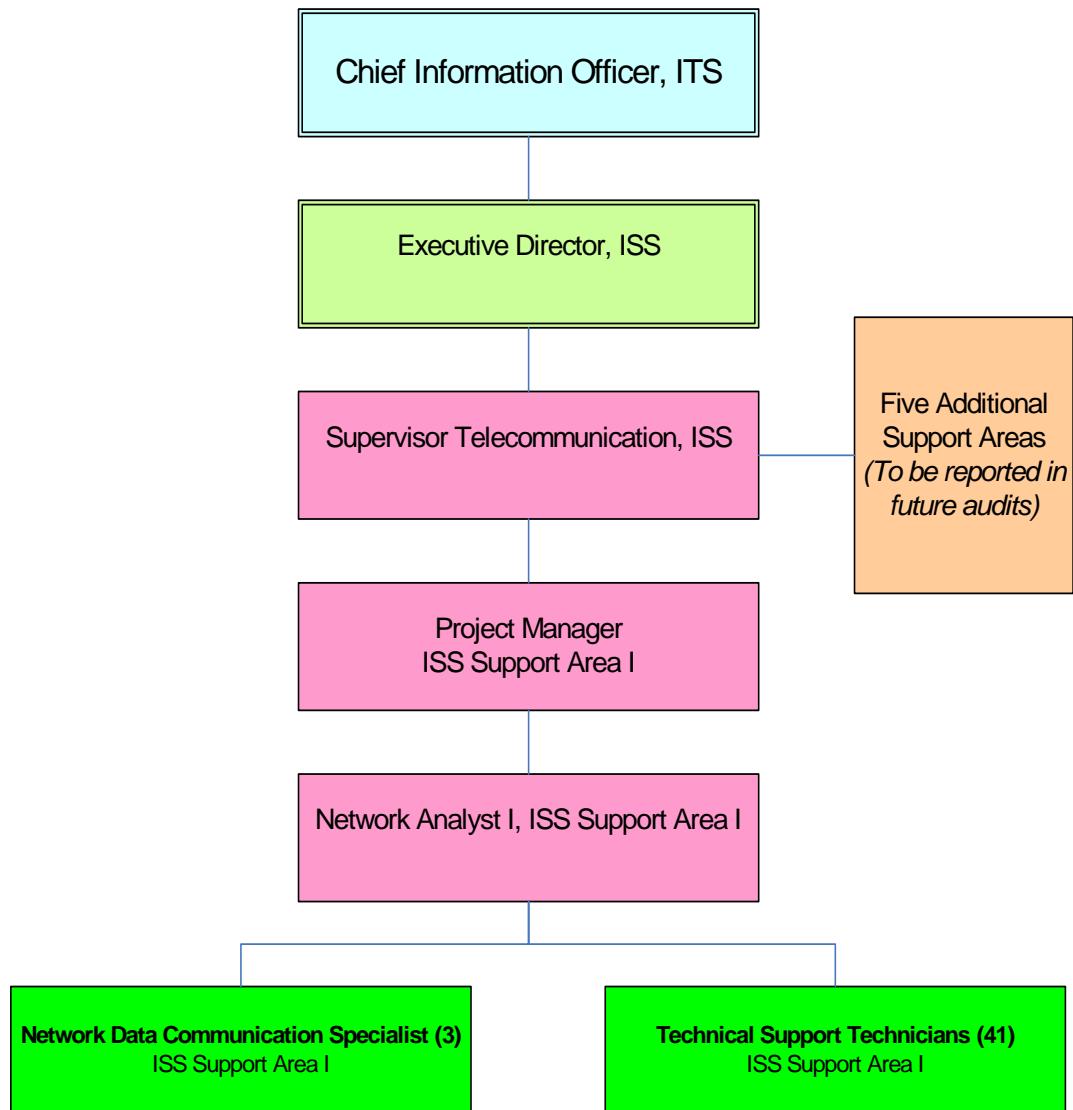
It should be noted that prior to the realignment described above, TSTs were classified as 12-month employees. TSTs now follow a 10-month work schedule similar to most school site personnel. Consequently, IT support resources have diminished significantly and have been compounded by a steady exodus of school site technical staff leaving the M-DCPS workforce.

Due to the sometimes unfamiliar nature of the issues being discussed, as well as the prolific use of acronyms when referring to technology, the following definitions are provided for the reader's reference:

AD	Active Directory (Microsoft ® terminology) – A database of computer and user accounts. A central component of the Windows platform, Active Directory provides the means to manage the identities and relationships that make up the network environments.
BIGFIX	Patch management and remote administration tool, which also provides condition reports of all computers that have connected to the DADESCHOOLS network within the prior 30 days.
DOMAIN	A collective group of computers, which are all members of the same “family”.
Group Policy	Centralized method of applying restrictions or conditions to a group of users or computers (Microsoft ® terminology).
IP Address	Internet Protocol or IP address is a unique number assigned to a computer that enables it to access network resources.
Local Administrator	A special account, which allows a user to have control over the computer, including modifying the computer's profile.
NSS	M-DCPS Network Security Standards document that delineates security guidelines for M-DCPS.
PC	Personal computer or workstation.
Server	Central repository, which stores and shares data on a network.
SOPHOS	The enterprise-level antivirus (AV) software product in use by the M-DCPS.
Tipping Point	Network intrusion prevention device.
WAP	Wireless Access Point

ORGANIZATIONAL CHART

Infrastructure and Systems Support (ISS) *Support Area I, (WL 9413)*



OBJECTIVES, SCOPE AND METHODOLOGY

In accordance with the approved Audit Plan for the 2010-11 Fiscal Year, we have performed an audit of network data and systems security at 20 (or 33%) of the 60 schools located within ISS Support Area I. The objectives of the audit were to determine whether adequate controls are in place to:

- Protect critical information;
- Protect supporting IT systems;
- Ensure adherence to the District's Network Security Standards (NSS); and
- Identify and apply industry best practices to the District's IT function.

The scope of this audit encompasses current practices and procedures followed by the schools within ISS Support Area I.

We performed the following procedures to satisfy our audit objectives:

- Analyzed site assessment of each school submitted by ISS Project Managers with input from TSTs, NDCS and NA and other data, and selected a sample of schools for review.
- Interviewed district staff identified in the organizational chart;
- Utilized software such as Active Directory, BigFix and other tools to mine for specific data;
- Reviewed required documentation related to district policies, personnel and network layouts;
- Examined and tested a random sample of servers and desktop computers at each location for compliance with the standards referred to in our audit objectives;
- Verified the installation and operation of required and optional equipment;
- Inspected physical storage facility where servers are housed; and
- Performed other audit procedures as deemed necessary.

We conducted this performance audit in accordance with generally accepted *Government Auditing Standards* issued by the Comptroller General of the United States of America. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

This audit included an assessment of applicable internal controls and compliance with the requirements of established policies, procedures and rules. Additionally, the findings and recommendations reflect general trends observed within the sample group reviewed rather than isolating individual school issues.

Our determination of each school's compliance or non-compliance with established standards, as well as the resulting findings and recommendations were assembled utilizing the following criteria applied to 19 areas of audit concerns:

- Is the M-DCPS Network Security Standards being followed?
- Are industry best practices being employed?
- What tools are available for detecting undesirable conditions?
- How difficult or time consuming is it to look for or monitor deficiencies?
- How difficult or time consuming is it to implement corrective actions?
- What is the risk to the District associated with non-compliance?
- Is technical staff aware of policies and procedures?

In assessing compliance with the aforementioned 19 areas of audit concerns, we applied our audit tests to either administrative and faculty computers only or to all (i.e., student, faculty and administrative) computers based on the applicability of each audit concern tested.

Throughout this report, references to 'best practices' primarily refer to established practices that were recommended in the State of Florida Auditor General Report No. 2007-005 – ***Selected State Agencies' Progress in Assessing Network and System Vulnerabilities***, *Information Technology Audit*, July 2006. However, we also refer to other generally recognized 'best or leading practices'.

FINDINGS AND RECOMMENDATIONS:

1. RECONCILE SCHOOL SITE ACTIVE DIRECTORY COMPUTER ACCOUNTS

Established Standards

The District utilizes a technology developed by the Microsoft Corporation called Active Directory (AD). Simply put, AD is a database housing an account for every computer on the network. Over time, with the addition, removal and servicing of computers, AD becomes populated with “orphaned” accounts that are not associated with a “live” computer. This results in thousands of unused or “orphaned” accounts remaining in the database.

BigFix is a tool that has been deployed to all district computers. It periodically reports to a central database and closely matches the actual number of “live” computers. Technical Support Technicians (TSTs) have access to BigFix reports, which can be used to reconcile AD.

It is a leading practice that AD be reconciled, thereby improving performance and providing a true representation of the actual computer population in each school and in the District as a whole. Knowing the true population of computers enhances accountability and control over software licenses.

Observed Practice

Our audit concluded that 13 of the 20 locations reviewed (or 65%) have not reconciled AD. The range of the delta for the number of computers in the AD library versus the BigFix library was from a low of 27 computers (11%) to a high of 440 computers (54%).

RECOMMENDATION:

- 1.1 Require TSTs to reconcile their assigned location(s) AD on a routine basis using BigFix as a baseline.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT’S RESPONSE:

ITS Audit Response:

- ITS concurs with this finding. In researching this issue, the following are some of the reasons we found for the AD counts to be greater than the Big Fix counts:
 - Computers with corrupted Big Fix and/or Sophos clients not showing on Big Fix counts.
 - Computers pending repair and/or service still showing in AD.
 - New computers deployment and imaging in progress.
 - Wireless labs and off-site loaner devices not being actively used when Big Fix reports run

ITS Standards Implemented to resolve the findings:

- Require TST to run Monthly Big Fix and AD reports in order to correlate reports and fix any corrupted clients in order to have less than a 10% delta.
- Require TST to document reasons for delta which can be provided to ITS and auditors on request.
- Require TST to run any unused wireless labs every few months in order for them to get their updates and be counted by Big Fix. Also require that all M-DCPS off-site devices be brought in once a month to connect to the network for updates.
- ITS will perform random audit to verify Standards and procedures are being followed.

2. ANTIVIRUS SOFTWARE NEEDS TO BE INSTALLED ON ALL COMPUTERS

Established Standards

Through memoranda from the Superintendent of Schools, all school and non-school site administrators are notified of revisions to the M-DCPS Network Security Standards (NSS) and of the need to fully comply with all district security initiatives and standards, in order to keep its network secure. According to the M-DCPS NSS 4.1.1.9, 5.0.8 and 5.0.17 and industry recommended best practices, antivirus (AV) software should be installed on all computers.

Observed Practice

Our review showed that all 20 schools audited maintained evidence of their employee's awareness of the M-DCPS NSS. Furthermore, all except for 2 of the 20 schools audited ensured that critical software updates or patches were installed on their computers. In addition, in order to access network resources and to receive district-deployed patches and software, PCs on the M-DCPS network must be members of a **domain** or "family" of computers. The computers tested at all 20 schools audited were members of the DADESCHOOLS domain on the date we visited those schools. However, four (4) of the 20 schools audited (or 20%) had computers that did not have the required AV software installed. We realize that 100% compliance at all schools is difficult to achieve; however, the number of instances of non-compliance appears to indicate a condition that affects a number of schools within ITS ISS Area I. Moreover, tools are readily available to detect and rectify this condition.

The District utilizes an AV solution called SOPHOS. AV software is a vital component needed to safeguard data, protect M-DCPS business processes and confidential student/employee information from viruses and other malicious threats. AV software is automatically deployed on the District's network via BigFix. Our test found that at 19 of the 20 schools audited, computers contained the current version of BigFix. BigFix is the patch management tool the District uses. This method of deployment significantly reduces labor and overhead that would otherwise be incurred with individual installation. Many TSTs rely exclusively on this method for AV installation.

TSTs have access to BigFix reports, which quickly identify PCs that are missing or indicating a problem with their AV software. This report allows technicians to pinpoint and address AV software issues very efficiently and keep vulnerability to a minimum by ensuring all computers are protected.

RECOMMENDATION:

- 2.1 Require TSTs to regularly review BigFix AV reports for all assigned locations and to address AV deficiencies.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Response:

- ITS concurs with this finding. In researching the issue we did not note any schools which did not have the required AV software installed. Only a few computers at some schools had corrupted Big Fix and/or Sophos clients which prevented them from receiving the latest AV updates. These corrupted machines are re-imaged or manually corrected in an on-going process as they appear.

ITS Standards Implemented to resolved findings:

- Require TST to run Monthly AV Reports utilizing Big Fix.
- Recommend implementing Window Update Services Server (WSUS) as backup to Big Fix.
- ITS will perform random audit to verify Standards and procedures are being followed.

3. COMPUTERS NEED TO BE PASSWORD-PROTECTED AFTER USER LOGIN

Established Standards

Section 4.1.1.10 of the NSS reads, in pertinent part:

“All administrative computers and server consoles that are used to access or control sensitive data must have a screen saver timeout and password after a specific period of inactivity or some other lockout mechanism to prevent unauthorized persons from accessing the data via the logged-in user’s account. The Windows timeout with password is available even if the specific application does not have one.”

Observed Practice

After authorized users logon to the MDCPS network, many district functions, network resources, and confidential data are made accessible. Unsupervised and unlocked computers pose a significant threat to the integrity of district information.

We examined a sample of administrative computers and found that at 12 of the schools visited (or 60%), timeouts with password protection after authorized login had not been enabled on all computers tested, leaving those unprotected computers vulnerable to tampering. Additionally, this function is being left to the discretion of individual users. Our experience finds that when left up to the user, implementation of this setting is generally ignored. Furthermore, tampering would be difficult to detect and may go undetected since changes are accomplished while logged in as an authorized user.

RECOMMENDATION:

- 3.1 Require TSTs to comply with the NSS and industry best practices by implementing a group policy that forces sensitive computers on the school’s network (teacher, server and administrative workstations) to automatically lock after a preset amount of user inactivity.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT’S RESPONSE:

Audit Response:

- ITS concurs with this finding. Although the time out policy was included in the GPOs, it was not applied to some servers because these servers had not rebooted in a very long time.

ITS Standards Implemented to resolved findings:

- The TST must reboot all servers on a schedule in order for all policies to take effect.
- Implement Group Policy to lock and/or log off user after 15 minutes of non active session.
- ITS will perform random audit to verify Standards and procedures are being followed.

4. NON-STANDARD LOCAL ADMINISTRATOR ACCOUNTS ARE FOUND THROUGHOUT SOME SCHOOLS' NETWORKS

Established Standards

The standard method for accessing District computers involves supplying a network user ID and password. This process grants or limits access to the computer and network resources based on permissions that have been applied to a user's account by a network administrator.

A **Local Administrator** (LA) login is a powerful account allowing complete and unrestricted access to a computer and all information contained therein. LA accounts are typically known only to the network manager and are used to install/uninstall software and hardware, and for troubleshooting purposes.

A second component related to LA access concerns LA Groups; (i.e., user accounts which are members of a **group** that has been given LA authority). Using **group accounts** to provide access instead of individual user accounts is an industry best practice and is required by NSS (4.1.1.13).

Observed Practice

Our audit found that although the computers tested at 18 of the 20 schools visited had the required minimum accounts or groups, 10 of those schools (or 50%) showed the presence of various non-standard LA accounts (*accounts with the same type of LA authority in addition to the required built-in account*) throughout the network. This practice significantly increases the risk of unauthorized access to systems, bypassing the controls of a standard network login. Furthermore, it also introduces the potential for non-technical users to perform unauthorized, unintended or harmful configuration.

In addition, at five (5) of the 20 schools audited (or 25%), LA access was being handled using standalone accounts. Four (4) of the 20 schools audited (or 20%) had both of the conditions described. By adding or removing users from groups, permissions are efficiently managed when a user's role changes.

RECOMMENDATIONS:

- 4.1 Require TSTs to verify and delete all non-standard LA accounts. Existing image files (deployable copies of hard drive installations) should be reviewed to ensure that non-standard LA accounts are not part of the image to prevent unintentional redistribution.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Response:

- ITS concurs with this finding. In researching this issue, we found that although some computers had multiple LA accounts, all were secured accounts. Also certain accounts that are associated with services running on servers require a dedicated account to run automated tasks. For example a backup server may require the local admin account to run if the Domain is not available. These "service accounts" are password protected and documented.

ITS Standards Implemented to resolved findings:

- All new image creation and deployment now includes our desktop standards and security permissions.
- We have implemented a standard where we manage user permissions utilizing AD and not local admin accounts wherever possible.
- ITS will perform random audit to verify Standards and procedures are being followed.

- 4.2 Require that all other LA-type access be managed through group memberships, not through individual accounts.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Response:

- ITS concurs with this finding. In researching this issue, we found that although some computers were found which had multiple LA accounts, all

were secured accounts. Also certain accounts that are associated with services running on servers require a dedicated account to run automated tasks. For example a backup server may require the local admin account to run if the Domain is not available. These accounts are password protected and documented.

ITS Standards Implemented to resolved findings:

- We have implemented a standard where we manage user permissions utilizing AD and not local admin accounts wherever possible.
- ITS will perform random audit to verify Standards and procedures are being followed.

**5. SOME COMPUTERS ARE
NAMED IN A MANNER THAT
INCREASES VULNERABILITY**

Established Standards

Computers must be given a unique name in order to function and to be recognized on the M-DCPS network. NSS 5.0.17 requires that a computer name begins with the four digit work location number. This rule helps to identify the location of a computer for troubleshooting purposes as well as aiding with monitoring and auditing purposes. In addition, an established school of thought within the IT community discourages naming computers in a manner that provides an easily traceable path the owner of the computers based upon their name, job title or function, etc.

Observed Practice

Our audit found that the computers tested at all 20 schools audited complied with the naming convention described in NSS 5.0.17. However, five (5) schools (25%) had computers that used the name of an individual or job title as part of the computer name. Workstations that are named according to user role (ex. 9131-Principal) or personal name (ex. 9131-JSmith) provide clues and facilitate targeted attacks.

RECOMMENDATION:

- 5.1 In order to enhance security, TSTs should be required to name computers using the work location's assigned number followed by generic information that is meaningful to a technician but is insignificant to an attacker. ITS should consider developing and implementing a District-wide protocol for the naming of computers that follows this recommendation.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Response:

- ITS concurs but notes that this is a new requirement. All desktops are now being named in accordance with the Computer Naming Standards which does not reflect the person's title or job description.

ITS Standards Implemented to resolved findings:

- ITS will perform random audit to verify Standards and procedures are being followed.

6. SERVERS NEED TO BE ROUTINELY BACKED UP

Established Standards

Servers are essentially upgraded computers equipped with redundancy components to protect against failure and act as a centralized network repository where users can store and access critical data. Routine backups are a necessary step towards restoring data in the event of a system failure. The District's NSS (4.1.1.7) and best practices recommend that servers be backed up periodically as part of an entity's disaster recovery routine.

Observed Practice

Our audit showed that all 20 schools visited maintained a written disaster recovery plan and documentation of their network layout. In addition, four (4) of the five (5) schools, which had retired computers during the year provided evidence that they had complied with the NSS hard drive degaussing requirement upon disposal of computers. However, Our review showed that 4 schools (20%) were not performing routine data backups of their servers as required by the M-DCPS NSS and typical disaster recovery plans.

RECOMMENDATION:

- 6.1 Require TSTs to comply with NSS 4.1.1.7 and best practices by performing routine backups of critical data to provide recourse in the event of hardware failure. In addition, backup procedures should be fully documented, with copies made available to the school Principal and the appropriate ITS Administrator.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Response:

- ITS concurs with this finding. All disaster recovery plans include backup procedures, but lack of funds has prevented many sites from purchasing the required hardware and or media to backup servers on a schedule. In the event that the automated backup failed or was not possible, the TSTs will perform a manual backup using alternative media or hardware provided by the site.

ITS Standards Implemented to resolved findings:

- Automated backup Standards in place.
- Notify Principals to purchase required equipment to perform backups.
- ITS will perform random audit to verify Standards and procedures are being followed.

7. PERFORM REVIEWS FOR THE PRESENCE OF UNAUTHORIZED WIRELESS ACCESS POINTS AND DOCUMENT THE RESULTS

Established Standards

When installed correctly, Wireless Access Points (WAPs) provide a simple and cost effective method of making network resources available. Information Technology Services (ITS) has developed an operating practice where TSTs are required to perform routine sweeps throughout their assigned campuses to detect the installation of unapproved WAPs. Results are to be documented and reported to the Principal and to an ITS Administrator for appropriate action, if necessary.

In addition, NSS 4.2, states in part that, "ITS must be informed of all District wireless installations. This includes school sites... Site supervisors and technicians should check that other staff does not install rogue devices without approval and/or correct security settings. These devices become open doors to hackers seeking to get into the network."

Observed Practice

Due to the relatively low cost and wide availability of these devices, WAPs are sometimes purchased and installed without the knowledge of school administrators or technicians. This creates a vulnerable entry point to the M-DCPS network that can be accessed by devices such as laptops, tablets and smart-phones. At three (3) of the 20 schools audited (or 15%), verification for unauthorized WAPs was not being performed.

RECOMMENDATION:

- 7.1 Require TSTs to comply with the NSS 4.2, by routinely performing sweeps for the presence of unauthorized WAPs and reporting documented results to the Principal and to the appropriate ITS Administrator.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Response:

ITS concurs with this finding. All sites have been performing wireless sweeps, but some had not been following the correct reporting procedures. All TSTs are now in compliance of this guideline.

ITS Standards Implemented to resolved findings:


- Wireless Scan procedure implemented.
- ITS will perform random audit to verify Standards and procedures are being followed.

MANAGEMENT'S RESPONSE

MEMORANDUM

May 10, 2011
DK #111/2010-2011

TO: Jose Montes-de-Oca, Chief Auditor
Office of Management and Compliance Audits

FROM: Debbie Karcher, Chief Information Officer
Information Technology Services 

SUBJECT: **RESPONSE TO OMCA DRAFT OF INFRASTRUCTURE & SYSTEMS
SUPPORT (ISS) AREA I-SELECTED SCHOOL SITES**

Below are the Information Technology Services (ITS) responses to the seven items on the ISS AREA I selected school sites field audit. It should be noted that it is very difficult to maintain an absolute, 100% secure posture in classrooms, especially considering that the student users we deal with every day are not only very tech savvy, but are often actively trying to evade our efforts. It should also be noted that there are 125,000 District-owned computers connected to the network, with many more personally-owned devices coming on-line all the time.

The school site computers' protective applications are merely the first line of defense in a many-layered approach to security. Computers that are breeched are quickly identified, isolated, shut down, and scheduled for cleaning. This protects the rest of the network and occurs because of our Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Nevertheless, ITS and the TSTs continue to strive to be 100% free of issues.

RECOMMENDATIONS:

- 1.1 Require TSTs to reconcile their assigned location(s) AD on a routine basis using BigFix as a baseline.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Reconcile school site active directory computer accounts.

ITS Audit Response:

- ITS concurs with this finding. In researching this issue, the following are some of the reasons we found for the AD counts to be greater than the Big Fix counts:
 - Computers with corrupted Big Fix and/or Sophos clients not showing on Big Fix counts.
 - Computers pending repair and/or service still showing in AD.

- New computers deployment and imaging in progress.
- Wireless labs and off-site loaner devices not being actively used when Big Fix reports run

ITS Standards Implemented to resolve the findings:

- Require TST to run Monthly Big Fix and AD reports in order to correlate reports and fix any corrupted clients in order to have less than a 10% delta.
- Require TST to document reasons for delta which can be provided to ITS and auditors on request.
- Require TST to run any unused wireless labs every few months in order for them to get their updates and be counted by Big Fix. Also require that all M-DCPS off-site devices be brought in once a month to connect to the network for updates.
- ITS will perform random audit to verify Standards and procedures are being followed.

2.1 Require TSTs to regularly review BigFix AV reports for all assigned locations and to address AV deficiencies.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Antivirus software needs to be installed on all computers.

Audit Response:

- ITS concurs with this finding. In researching the issue we did not note any schools which did not have the required AV software installed. Only a few computers at some schools had corrupted Big Fix and/or Sophos clients which prevented them from receiving the latest AV updates. These corrupted machines are re-imaged or manually corrected in an on-going process as they appear.

ITS Standards Implemented to resolved findings:

- Require TST to run Monthly AV Reports utilizing Big Fix.

- Recommend implementing Window Update Services Server (WSUS) as backup to Big Fix.
- ITS will perform random audit to verify Standards and procedures are being followed.

3.1 Require TSTs to comply with the NSS and industry best practices by implementing a group policy that forces sensitive computers on the school's network (teacher, server and administrative workstations) to automatically lock after a preset period of user inactivity.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Computers need to be password-protected after user login

Audit Response:

- ITS concurs with this finding. Although the time out policy was included in the GPOs, it was not applied to some servers because these servers had not rebooted in a very long time.

ITS Standards Implemented to resolved findings:

- The TST must reboot all servers on a schedule in order for all policies to take effect.
- Implement Group Policy to lock and/or log off user after 15 minutes of non active session.
- ITS will perform random audit to verify Standards and procedures are being followed.

4.1 Require TSTs to verify and delete all non-standard LA accounts. Existing image files (deployable copies of hard drive installations) should be reviewed to ensure that non-standard LA accounts are not part of the image to prevent unintentional redistribution.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Non-standard local administrator accounts are found throughout some schools' networks.

Audit Response:

- ITS concurs with this finding. In researching this issue, we found that although some computers had multiple LA accounts, all were secured accounts. Also certain accounts that are associated with services running on servers require a dedicated account to run automated tasks. For example a backup server may require the local admin account to run if the Domain is not available. These "service accounts" are password protected and documented.

ITS Standards Implemented to resolved findings:

- All new image creation and deployment now includes our desktop standards and security permissions.
- We have implemented a standard where we manage user permissions utilizing AD and not local admin accounts wherever possible.
- ITS will perform random audit to verify Standards and procedures are being followed.

4.2 Require that all other LA - type access be managed through group memberships, not through individual accounts.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Non-Standard local administrator accounts are found throughout some schools' networks.

Audit Response:

- ITS concurs with this finding. In researching this issue, we found that although some computers were found which had multiple LA accounts, all were secured

accounts. Also certain accounts that are associated with services running on servers require a dedicated account to run automated tasks. For example a backup server may require the local admin account to run if the Domain is not available. These accounts are password protected and documented.

ITS Standards Implemented to resolved findings:

- We have implemented a standard where we manage user permissions utilizing AD and not local admin accounts wherever possible.
- ITS will perform random audit to verify Standards and procedures are being followed.

- 5.1 In order to enhance security, TSTs should be required to name computers using the work location's assigned number followed by generic information that is meaningful to a technician but is insignificant to an attacker. ITS should consider developing and implementing a District-wide protocol for the naming of computers that follows this recommendation.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Some computers are named in a manner that increases vulnerability.

Audit Response:

- ITS concurs but notes that this is a new requirement. All desktops are now being named in accordance with the Computer Naming Standards which does not reflect the person's title or job description.

ITS Standards Implemented to resolved findings:

- ITS will perform random audit to verify Standards and procedures are being followed.

- 6.1 Require TSTs to comply with NSS 4.1.1.7 and best practices by performing routine backups of critical data to provide recourse in the event of hardware failure. In addition, backup procedures should be fully documented, with copies made available to the school Principal and the appropriate ITS Administrator.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Servers need to be routinely backed up.

Audit Response:

- ITS concurs with this finding. All disaster recovery plans include backup procedures, but lack of funds has prevented many sites from purchasing the required hardware and or media to backup servers on a schedule. In the event that the automated backup failed or was not possible, the TSTs will perform a manual backup using alternative media or hardware provided by the site.

ITS Standards Implemented to resolved findings:

- Automated backup Standards in place.
- Notify Principals to purchase required equipment to perform backups.
- ITS will perform random audit to verify Standards and procedures are being followed.

7.1 Required TSTs to comply with NSS 4.2 by routinely performing sweeps for the presence of unauthorized WAPs and reporting the documented results to the Principal and to the appropriate ITS Administrator.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Perform reviews for the presence of unauthorized wireless access points and document the results.

Audit Response:

ITS concurs with this finding. All sites have been performing wireless sweeps, but some had not been following the correct reporting procedures. All TSTs are now in compliance of this guideline.

Memorandum

SUBJECT: RESPONSE TO OMCA DRAFT OF INFRASTRUCTURE & SYSTEMS SUPPORT (ISS) AREA I-
SELECTED SCHOOL SITES

Page 7

ITS Standards Implemented to resolved findings:

- Wireless Scan procedure implemented.
- ITS will perform random audit to verify Standards and procedures are being followed.

DK:jp

cc: Mr. Trevor Williams
Mr. Javier Perez
Mr. James O'Donnell

The School Board of Miami-Dade County, Florida, adheres to a policy of nondiscrimination in employment and educational programs/activities and programs/activities receiving Federal financial assistance from the Department of Education, and strives affirmatively to provide equal opportunity for all as required by:

Title VI of the Civil Rights Act of 1964 - prohibits discrimination on the basis of race, color, religion, or national origin.

Title VII of the Civil Rights Act of 1964, as amended - prohibits discrimination in employment on the basis of race, color, religion, gender, or national origin.

Title IX of the Education Amendments of 1972 - prohibits discrimination on the basis of gender.

Age Discrimination in Employment Act of 1967 (ADEA), as amended - prohibits discrimination on the basis of age with respect to individuals who are at least 40.

The Equal Pay Act of 1963, as amended - prohibits sex discrimination in payment of wages to women and men performing substantially equal work in the same establishment.

Section 504 of the Rehabilitation Act of 1973 - prohibits discrimination against the disabled.

Americans with Disabilities Act of 1990 (ADA) - prohibits discrimination against individuals with disabilities in employment, public service, public accommodations and telecommunications.

The Family and Medical Leave Act of 1993 (FMLA) - requires covered employers to provide up to 12 weeks of unpaid, job-protected leave to "eligible" employees for certain family and medical reasons.

The Pregnancy Discrimination Act of 1978 - prohibits discrimination in employment on the basis of pregnancy, childbirth, or related medical conditions.

Florida Educational Equity Act (FEEA) - prohibits discrimination on the basis of race, gender, national origin, marital status, or handicap against a student or employee.

Florida Civil Rights Act of 1992 - secures for all individuals within the state freedom from discrimination because of race, color, religion, sex, national origin, age, handicap, or marital status.

School Board Rules 6Gx13- 4A-1.01, 6Gx13- 4A-1.32, and 6Gx13- 5D-1.10 - prohibit harassment and/or discrimination against a student or employee on the basis of gender, race, color, religion, ethnic or national origin, political beliefs, marital status, age, sexual orientation, social and family background, linguistic preference, pregnancy, or disability.

Veterans are provided re-employment rights in accordance with P.L. 93-508 (Federal Law) and Section 295.07 (Florida Statutes), which stipulate categorical preferences for employment.

INTERNAL AUDIT REPORT

Network and Information Security Information Technology Services Infrastructure and Systems Support Area I – Selected School Sites



**MIAMI-DADE COUNTY PUBLIC SCHOOLS
Office of Management and Compliance Audits
1450 N.E. 2nd Avenue, Room 415
Miami, Florida 33132**
